PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-306273
(43)Date of publication of application : 02.11.2001

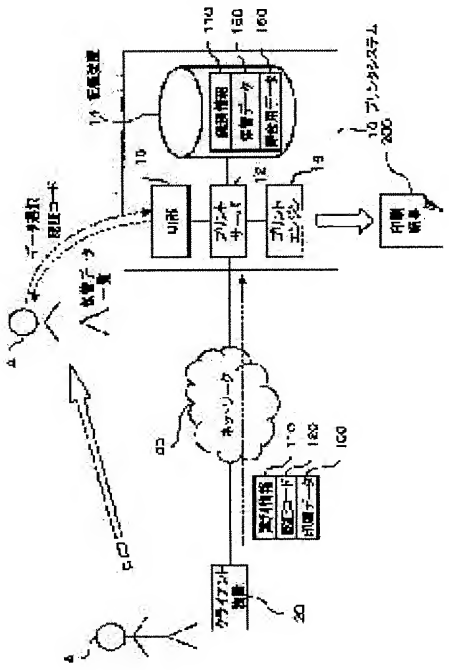
(51)Int.Cl. G06F 3/12
B41J 5/30
H04L 9/32

(21)Application number : 2000-125801
(22)Date of filing : 26.04.2000

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : NAGAYAMA HIRONOBU
TAKEDA MASARU
GENDA KOHEI
TOKI YASUYUKI

(54) METHOD FOR CONTROLLING IMAGE OUTPUT AND DEVICE FOR OUTPUTTING PICTURE

(57)Abstract:
PROBLEM TO BE SOLVED: To protect the secret of data preserved in an image outputting device.
SOLUTION: A client device 20 transmits print data 100 and an authentication code 120 to a printer system 10. A print server 12 of the printer system 10 generates data 160 for collation from the print data 100, and enciphers the print data 100 by the authentication code 120 for generating preservation data 150, and preserves the preservation data 150 and the data 160 for collation in a storage device 14 by making those data correspond to each other. When a user selects the preservation data 150 by a UI part 18, and inputs the authentication code, a printer server 12 decodes the preservation data 150 by using the authentication code as a key, and judges whether or not the preservation data 150 are correctly decoded by referring to the data 160 for collation. Then, when the preservation data 150 are correctly decoded, the decoded result is printed by a print engine 16.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A generating picture job which a client published is once kept to an image output device, It is a picture output control method which waits for and carries out the generating picture of said kept job for output instruction from a user, A picture output control method which should encipher said generating picture job kept to said image output device, and said image output device decrypts data of the enciphered generating picture job by a decryption key inputted from a user on the occasion of output instruction of a generating picture job, and performs image output processing.
[Claim 2]The picture output control method according to claim 1 transmitting a cryptographic key to said image output device with said generating picture job from said client, and said image output device's enciphering the generating picture job by the cryptographic key, and keeping it.
[Claim 3]The picture output control method according to claim 1 only when it judges whether a decryption result of said generating picture job is the right and said image output device is judged [a decryption result] to be the right, wherein it performs an output process.
[Claim 4]The picture output control method according to claim 3, wherein said image output device creates data for collation for a judgment of a decryption result of being the right and keeps this data with an encryption result of said generating picture job from data of that job in the case of encryption of said generating picture job.
[Claim 5]The picture output control method according to claim 3 carrying out possible [of the deletion of a generating picture job which was being kept] only when said decryption result is judged to be the right.
[Claim 6]The picture output control method according to claim 1, wherein said image output device enciphers and keeps a generating picture job received from said client and it notifies a decryption key of the encryption result to said client.
[Claim 7]An image output device comprising:
A means to receive a generating picture job and an authorization code from a client.
A means to encipher by the authorization code and to keep the generating picture job.
A means to receive an input of an authorization code from a user in connection with output instruction to said kept job.
An output control means which decrypts said job for output instruction and performs a generating picture by an inputted authorization code based on the decryption result.

[Claim 8]An image output device comprising:
A means to receive a generating picture job from a client.
A means to notify a decryption key of the encryption result to said client while enciphering and keeping the generating picture job.
A means to receive an input of a decryption key from a user in connection with output instruction to said kept job.
An output control means which decrypts said job for output instruction and performs a generating picture by an inputted decryption key based on the decryption result.

[Claim 9]An image output device which will process the job and will perform a generating picture if a generating picture job is received and kept from a client via a network characterized by comprising the following and output instruction occurs from a user.
A means to keep a generating picture job.
A means to receive selection of an output object out of a kept generating picture job.
A means to judge whether a selected generating picture job is enciphered.
An output control means which requires an input of a decryption key, decodes the job by a decryption key inputted according to this, and performs a generating picture using the decryption result when a selected generating picture job is enciphered.

[Claim 10]An image output device given in either from claim 7 only when it judges whether said decryption result is the right and said output control means is judged [a decryption result] to be the right, wherein it performs an output process to claim 9.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the method of the output control of the job when a generating picture job is transmitted from a client via a network to a remote image output device.
[0002]
[Description of the Prior Art]an output becoming that it is indistinguishable from others' printout and hard to find it, when performing a printout to a remote printer via a network, or an output being seen by others by the time a user goes to take even a printer, or losing **** -- etc. -- the problem is pointed out from the former.
[0003]As conventional technology for solving such a problem, it registers for the print server as a user beforehand, and the method which performs user authentication in a print server and performs a printout is known well. For example, in the method indicated by JP,8-256239,A, if a user name and a password are entered with a digital composite machine, the composite machine will log in to a user's PC (personal computer), print data will be acquired, and a printout will be performed. In art given in JP,11-305968,A, the print server accumulates the print data received from the client, and if the input of just certification information is received from a user about the data, it will carry out the printout of the data.
[0004]Attestation ID is added to the print job sent to a print server as conventional technology of another method, and the method which makes a printout possible in inputting the attestation ID into a print server is known. There is art shown, for example in each gazette of JP,9-212317,A, JP,10-16355,A, JP,11-305968,A, and JP,11-15609,A in such a method.
[0005]
[Problem(s) to be Solved by the Invention]Since a printout was not performed from a print server unless it passes through attestation, each above-mentioned conventional technology was effective in respect of calling it the security of a printed result. However, in order that each of each above-mentioned conventional technologies may keep the print data sent from the client as it is in a print server, it may have been tried to look into the kept print data.
[0006]This invention is made in order to solve such a problem, and it is a thing.
The purpose is to provide the picture output control method and device which realize security of the data kept to the image output device of **.

[0007]
[Means for Solving the Problem]In order to solve such a problem, it is made to keep a generating picture job which performed encryption processing to image output devices, such as a printer, in this invention. And in the case of generating pictures, such as printing, kept job data are decrypted by a decryption key which a user inputted, and an output process is performed.
[0008]Here, it judges whether a decryption result is the right and a useless output can be prevented because it is made not to perform an output process in not being right. A judgment of propriety of a decryption result creates and keeps data for collation from data of the original job in the case of encryption, for example, It can carry out by comparing a decryption result with the

data for collation, or adding data for collation to data of a job, enciphering, and investigating whether it is a decryption result and the data for collation is decoded correctly.
[0009]
[Embodiment of the Invention]Hereafter, an embodiment of the invention (henceforth an embodiment) is described based on a drawing.
[0010][Embodiment 1] Drawing 1 is a figure for describing a 1st embodiment of this invention.
[0011]In this system, the printer system 10 as an image output device is a common printer system put, for example on a print shop, an office, etc., and contains the print server 12, the memory storage 14, the print engine 16, and the UI (user interface) section 18.
[0012]The print server 12 is a device which controls overall processing of the printer system 10. In addition to general processing capabilities, such as registration of the printing directions from the client apparatus 20, scheduling of a print job, conversion in the form of print data which can be printed, the print server 12 is provided with the function to encipher and keep print data to the memory storage 14. The memory storage 14 is a device which accumulates the print data etc. which were received from the client apparatus 20. The print engine 16 is a device which prints print data on paper etc. The UI section 18 is a device which provides an operation menu, a status display, etc. of the printer system 10, and receives an indicating input etc. to a user.
[0013]The printer system 10 has the function to keep the print data 100 received from the client apparatus 20 until the output instruction from a user occurs. Here, in this embodiment, security of the print data under storage is planned by enciphering and keeping them rather than keeping print data as it is. The print server 12 performs encryption processing and the authorization code 120 supplied from the client apparatus 20 is used for the encryption key for encryption.
[0014]When the user A is going to do the printout of the print data 100 from the printer system 10 and it desires security of print data, he sets up the authorization code 120. Any of the method which the user A itself inputs, and the method which the client apparatus 20 generates automatically according to a user's directions may be sufficient as setting out of the authorization code 120. The set-up authorization code 120 matches with the print data 100, and is transmitted to the printer system 10. The identification information 110 is added to the print data 100 transmitted. The title of the print data 100, etc. are information for the user A to identify the print data 100, and this identification information 110 is set up irrespective of the existence of setting out of the authorization code 120, for example.
[0015]In the printer system 10 which received the print data 100 from the client apparatus 20, the print server 12 memorizes these print data 100 to the memory storage 14 with the corresponding identification information 110. This procedure is shown in drawing 2.
[0016]The print server 12 is usually a reception waiting state of the data of the print data 100, the identification information 110, and authorization code 120 grade (S10, S12). Reception of the print data 100 will investigate whether the authorization code 120 accompanies (S14). If there is no authorization code 120, the print server 12 is matched with the identification information 110, will use the print data 100 as the stored data 150 as it is, and will keep them to the memory storage 14 (S24). (since I hear that the user is not demanding security)
[0017]If there is the authorization code 120, the print server 12 will judge next whether it is data of PDL (Page Description Language) which the print data 100 can process with the print engine 16 (S16). If this decision result is No, the print server 12 will change those print data 100 into PDL (S18). This conversion is unnecessary if the print data 100 are PDL.
[0018]Next, the print server 12 creates the data 160 for collation from the print data of PDL, matches with the identification information 110 and saves (S20). The data 160 for collation creates what extracted predetermined parts (the portion which is not related to a printing content is desirable), such as a header of the PDL data, the check sum value of the PDL data, etc. based on a predetermined rule from the PDL data. And using the authorization code 120 as a key, the print data of PDL are enciphered (S22), and the enciphered data is used as the stored data 150, is matched with the identification information 110, and is kept to the memory storage 14 (S24). Completion of storage will cancel the original print data 100 and the authorization code 120.
[0019]Next, processing when doing in this way and carrying out the printout of the kept data 150

is explained with reference to drawing 3.
[0020]First, the print server 12 displays the list of the identification information 110 of the stored data 150 currently kept in the memory storage 14 on the UI section 18 (S30). The user A who came chooses and directs data to carry out a printout out of the list display in the UI section 18 till the place of the printer system 10 (S32). According to this, the print server 12 performs the acknowledgment indicator of a start of printing in the UI section 18, and if the data may be satisfactory for a user, he will input that into the UI section 18 (S34).
[0021]If a user checks, the print server 12 will confirm whether to be data in which the selected stored data 150 is enciphered (S36). If not enciphered, the print server 12 passes the stored data to the print engine 16 as it is, and carries out a printout (S44). If enciphered, the print server 12 will perform the display to which the input of an authorization code is urged in the UI section 18, and will receive the input of the authorization code from a user to it (S38).
[0022]The method which forms the reader which a user makes the authorization code portable storage media, such as an IC card and a memory card, or other than a method performed by a manual entry memorize by keypad, a touch panel, etc., and reads the storage to the printer system 10 is also preferred for the input method of an authorization code.
[0023]If an authorization code is inputted, the print server 12 will decrypt the stored data 150 using the code (S40). And the data 160 for collation which was being kept corresponding to the stored data 150 and its decoding result are compared, and it confirms whether decoded correctly or not (S42). If not decoded correctly, it returns to S38 and an authorization code is reinputted. If decoded correctly, the data (data of PDL) of the decoding result will be passed to the print engine 16, and a printout will be made to perform as a result of collation (S44). Thereby, the printed result 200 is obtained.
[0024]It is asked after the printout of S44 whether the print server 12 cancels the stored data 150 which carried out the printout to a user via the UI section 18 (S46). In that there is a schedule of reuse of the stored data 150 etc., the user should just input directions of the purport that it does not cancel. When there are directions of cancellation, the print server 12 deletes the stored data 150 (and the corresponding identification information 110 and matching data 160 (supposing it is)) from the memory storage 14 (S48). Deletion will not be performed if there are directions of the purport that it does not cancel. In the case of the system installed in a print shop etc. for the use in an office building etc. although it is useful, it is unnecessary to enable it to leave the stored data 150.
[0025]It may set up with the client apparatus 20, may add and transmit to the print data 100, and may enable it to input the printing attributes at the time of a printout (number of copies, one side/both sides, etc.), for example after an attestation (decoding) success etc. by the printer system 10 side.
[0026]As explained above, since the print data 100 can be enciphered and kept to the printer system 10 according to the system of this embodiment, even if it should try to look into the data under storage, there is no possibility that the contents may be known. Since a printout is not performed unless stored data is correctly decoded by the right authorization code, the structure of this embodiment has also achieved the function of the user authentication at the time of output instruction. As [delete / a printout is carried out with the decoding result which is not right, and / since a printout is not performed and cancellation of stored data is not performed, either, unless it is decoded correctly / stored data]
[0027]In the above example, although the data 160 for collation was created from the print data (PDL) before encryption, the data 160 for collation is completely generated automatically independently, and it may be enciphered as print data by adding this to print data. The data for collation is made into a fixed value, and this may be added to print data and it may encipher. In this case, it is not necessary to match the data for collation with the stored data 150, and to save it.
[0028]In the above example, although encryption and decryption were performed by the same authorization code, if a public-key crypto system etc. are used, the key of encryption and the key of decryption can also be made separate.
[0029]In the above example, after the print server 12 changed the received print data 100 into

PDL which can process the print engine 16, encryption for storage was performed, but it is also preferred to encipher and keep the received print data 100 by the authorization code 120. In this case, after a user's authorization code input performs decoding processing, conversion to PDL is performed.

[0030][Embodiment 2] The above-mentioned Embodiment 1 enciphered print data by the printer system 10 side. On the other hand, in this embodiment, the method which keeps the data enciphered by the client apparatus 20 side to the printer system 10 was adopted.

[0031]The key map of the system of this embodiment is shown in drawing 4. According to this embodiment, the same cipher system (algorithm) as the client apparatus 20 and the printer system 10 is carried. And the user A sends the encryption data 180 obtained by enciphering the print data using a desired authorization code on the client apparatus 20 to the printer system 10, when it desires security of print data.

[0032]For the check of the decoding result by the side of the printer system 10, the data 160 for collation of a checksum etc. is added to the encryption data 180 to transmit, and also the identification information 110 and the authentication flag 170 are added to it. The authentication flag 170 is a flag which shows whether the print data to transmit are the encryption data 180 of what requires attestation, or it is data of PDL or application which is not enciphered. This is used in order to distinguish whether decoding processing is required for the data which the printer system 10 received. If the printer system 10 can distinguish the necessity of decoding processing by a file name and other attribution information, the authentication flag 170 has it.

[unnecessary]

[0033]Although the graphic display was omitted in drawing 4, when the print data transmitted from the client apparatus 20 are things without the necessity for security, the data 160 for collation is not added but the authentication flag 170 is set as the value which shows attestation (decoding and collation) needlessness.

[0034]From the client apparatus 20, the print server 12 which received the data of the printing request keeps those information to the memory storage 14. And the list of the identification information 110 of these stored data is displayed on the UI section 18, and it waits for selection from a user.

[0035]When a user chooses data, the print server 12 investigates the authentication flag 170 of the data. As a result, if attestation is unnecessary, the data will be changed into the form of PDL which can process the print engine 16, and a printout will be carried out from the print engine 16. On the other hand, if attestation is required, the input of an authorization code will be demanded from a user and the encryption data 180 will be decrypted by using as a key the authorization code inputted according to this. And it is inspected using the data 160 for collation whether the decoding result is a right thing. Henceforth, the same processing as Embodiment 1 is performed, and, as for a right case, a printout is performed for a decoding result.

[0036]Thus, in this embodiment, since it is not necessary to pass an authorization code (encryption key) directly to the printer system 10, security improves more.

[0037][Embodiment 3] Each above embodiment had set up the authorization code (encryption key) by the user side. On the other hand, according to this embodiment, an authorization code is set up by the printer system 10 side, and the method which notifies this to the user side is taken. Hereafter, a user has the personal digital assistant 20a as a client apparatus, and the example in the case of directing printing etc. using an E-mail is described.

[0038]A user sends E-mail 300 having contained the (1) print data 302 to the printer system 10 from the personal digital assistant 20a to print. The print data 302 are built into E-mail 300, for example in forms, such as the text of an E-mail, and an attached file.

[0039]The print server 12 of the printer system 10 which received this gives the authorization code 312 and the identification information 314 to a printing request with the E-mail 300. And like Embodiment 1, the print server 12 generates the data 360 for collation from the print data 302 in E-mail 300, matches this with the identification information 314, and memorizes it to the memory storage 14. By the given authorization code 312, the print server 12 enciphers the print data 302, matches them with the identification information 314 by using the encryption result as the stored data 350, and is kept to the memory storage 14. And the (2) print server 12 replies E-

mail 310 having contained the identification information 314 and the authorization code 312 to the personal digital assistant 20a of transmitting [printing request mail] origin. This mail 310 may contain the message of the purport that the printer system 10 received the printing request.

[0040]And if a user moves till the place of the printer system 10, he will send a reply from the personal digital assistant 20a to E-mail 310 from the printer system 10 like (3) points. If it is set as the e-mail system which the personal digital assistant 20a carries leave the original message to mail of a reply, the authorization code 312 and the identification information 314 will be automatically included in E-mail 320 replied. The user does not have to do the manual entry of these authorization codes 312 anew.
[0041]The print server 12 which received this mail 320 extracts the identification information 314 and the authorization code 312 from that mail 320, and picks out the stored data 350 and the data 360 for collation corresponding to that identification information 314 from the memory storage 14. And the print server 12 decodes the authorization code 312 for the stored data 350 as a key, and judges the propriety of the decoding result with the data 360 for collation. And a decoding result makes the print engine 16 print to a right case, and when a decoding result is not right, the mail which notifies the purport of an error to a user is transmitted.
[0042]Thus, in this embodiment, while the same effect as embodiment 1 grade is acquired, the time and effort of an input of the user in the case of output instruction can be saved by using the structure of an E-mail. Even standard mailer software should just be carried in users' device, and it is not necessary to provide the special hardware and software for this structure in it.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a figure for explaining the system of Embodiment 1.
[Drawing 2]It is a flow chart which shows the operation at the time of the data receiving of a print server.
[Drawing 3]It is a flow chart which shows the operation at the time of output instruction reception of a print server.
[Drawing 4]It is a figure for explaining the system of Embodiment 2.
[Drawing 5]It is a figure for explaining the system of Embodiment 3.
[Description of Notations]
10 A printer system and 12 [A network, 100 print data, and 110 / Identification information, 120 authorization codes, 150 stored data, and 160 / Data for collation.] A print server and 14 Memory storage and 16 Print engine, the 18 UI section, 20 client apparatus, and 30

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－306273
（P2001－306273A）
(43)公開日　平成13年11月２日(2001.11.2)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　3/12		Ｇ０６Ｆ　3/12	Ａ	２Ｃ０８７
Ｂ４１Ｊ　5/30		Ｂ４１Ｊ　5/30	Ｚ	５Ｂ０２１
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｊ１０４
				９Ａ００１

審査請求　未請求　請求項の数10　ＯＬ　（全８頁）

(21)出願番号　特願2000－125801(P2000－125801)

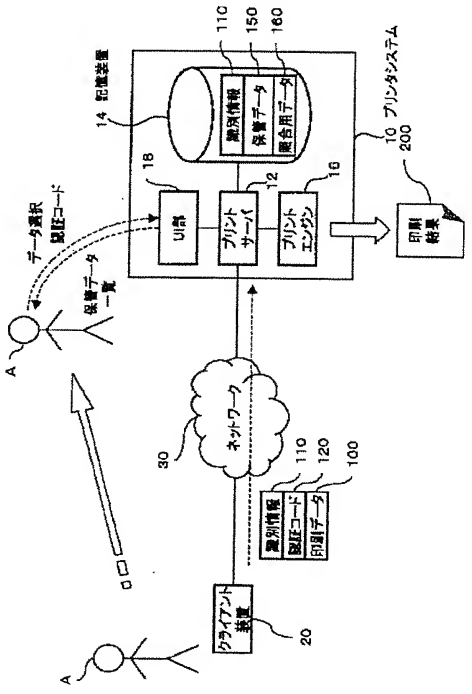
(22)出願日　平成12年４月26日(2000.4.26)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　永山　博信
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル
富士ゼロックス株式会社内
(72)発明者　武田　優
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル
富士ゼロックス株式会社内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

最終頁に続く

(54)【発明の名称】　画像出力制御方法及び画像出力装置

(57)【要約】
【課題】　画像出力装置に保管したデータの秘密を保護する。
【解決手段】　クライアント装置２０はプリンタシステム１０に対し、印刷データ１００と共に認証コード１２０を送信する。プリンタシステム１０のプリントサーバ１２は、受信した印刷データ１００から照合用データ１６０を生成し、更にその印刷データ１００を認証コード１２０により暗号化して保管データ１５０を生成し、それら保管データ１５０及び照合用データ１６０を互いに対応づけて記憶装置１４に保管する。ユーザがＵＩ部１８にて保管データ１５０を選択し、認証コードを入力すると、プリンタサーバ１２はその認証コードをキーとしてその保管データ１５０を復号し、正しく復号できたか否かを照合用データ１６０を参照して判定する。そして、正しく復号できていたら、その復号結果をプリントエンジン１６に印刷させる。



1

【特許請求の範囲】

【請求項１】　クライアントが発行した画像出力ジョブを画像出力装置にいったん保管し、保管した前記ジョブをユーザからの出力指示を待って画像出力する画像出力制御方法であって、

前記画像出力装置に保管する前記画像出力ジョブを暗号化したものとし、

前記画像出力装置は、ユーザから画像出力ジョブの出力指示の際に入力された復号キーにより、暗号化されたその画像出力ジョブのデータを復号化して画像出力処理を行う、

画像出力制御方法。

【請求項２】　前記クライアントから前記画像出力ジョブとともに暗号キーを前記画像出力装置に送信し、

前記画像出力装置は、その暗号キーによりその画像出力ジョブを暗号化して保管することを特徴とする請求項１記載の画像出力制御方法。

【請求項３】　前記画像出力装置は、前記画像出力ジョブの復号化結果が正しいか否かを判定し、復号化結果が正しいと判定された場合にのみ、出力処理を行うことを特徴とする請求項１記載の画像出力制御方法。

【請求項４】　前記画像出力装置は、前記画像出力ジョブの暗号化の際、そのジョブのデータから、復号化結果が正しいか否かの判定のための照合用データを作成し、このデータを前記画像出力ジョブの暗号化結果と共に保管することを特徴とする請求項３記載の画像出力制御方法。

【請求項５】　前記復号化結果が正しいと判定された場合のみ、保管していた画像出力ジョブの削除を可能することを特徴とする請求項３記載の画像出力制御方法。

【請求項６】　前記画像出力装置は、前記クライアントから受信した画像出力ジョブを暗号化して保管すると共に、前記クライアントに対してその暗号化結果の復号キーを通知することを特徴とする請求項１記載の画像出力制御方法。

【請求項７】　クライアントから画像出力ジョブ及び認証コードを受信する手段と、

その画像出力ジョブをその認証コードにより暗号化して保管する手段と、

保管した前記ジョブに対する出力指示に伴い、ユーザから認証コードの入力を受け付ける手段と、

入力された認証コードにより、出力指示対象の前記ジョブを復号化し、その復号化結果に基づき画像出力を行う出力制御手段と、

を含む画像出力装置。

【請求項８】　クライアントから画像出力ジョブを受信する手段と、

その画像出力ジョブを暗号化して保管するとともに、その暗号化結果の復号キーを前記クライアントに通知する手段と、

2

保管した前記ジョブに対する出力指示に伴い、ユーザから復号キーの入力を受け付ける手段と、

入力された復号キーにより、出力指示対象の前記ジョブを復号化し、その復号化結果に基づき画像出力を行う出力制御手段と、

を含む画像出力装置。

【請求項９】　ネットワークを介してクライアントから画像出力ジョブを受け付けて保管し、ユーザから出力指示があるとそのジョブを処理して画像出力を行う画像出力装置であって、

画像出力ジョブを保管する手段と、

保管された画像出力ジョブの中から出力対象の選択を受け付ける手段と、

選択された画像出力ジョブが暗号化されているか否かを判定する手段と、

選択された画像出力ジョブが暗号化されている場合、復号キーの入力を要求し、これに応じて入力された復号キーによりそのジョブを復号し、その復号化結果を用いて画像出力を行う出力制御手段と、

を含む、画像出力装置。

【請求項１０】　前記出力制御手段は、前記復号化結果が正しいか否かを判定し、復号化結果が正しいと判定された場合にのみ、出力処理を行うことを特徴とする請求項７から請求項９までのいずれかに記載の画像出力装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クライアントから遠隔の画像出力装置に対してネットワークを介して画像出力ジョブを送信したときのそのジョブの出力制御の方法に関する。

【０００２】

【従来の技術】ネットワークを介して遠隔のプリンタに印刷出力を行う場合、出力結果が他人の印刷出力に紛れて見つけにくくなったり、ユーザがプリンタまで取りに行くまでの間に出力結果が他人に見られたり紛失したりなどの問題が従来から指摘されている。

【０００３】このような問題を解決するための従来技術として、プリントサーバに予めユーザ登録をしておき、プリントサーバにてユーザ認証を行って印刷出力を行う方式がよく知られている。例えば、特開平８－２５６２３９号公報に開示された方式では、デジタル複合機でユーザ名及びパスワードを入力すると、その複合機がユーザのＰＣ（パーソナルコンピュータ）にログインして印刷データを取得し、印刷出力を行う。また特開平１１－３０５９６８号公報記載の技術では、プリントサーバはクライアントから受信した印刷データを蓄積しておき、そのデータについてユーザから正当な認証情報の入力を受け付けると、そのデータを印刷出力する。

【０００４】また、別の方式の従来技術として、プリン

トサーバに送る印刷ジョブに認証ＩＤを付加し、プリントサーバにその認証ＩＤを入力することで印刷出力を可能にする方式が知られている。このような方式には、例えば特開平９－２１２３１７号、特開平１０－１６３５５号、特開平１１－３０５９６８号、特開平１１－１５６０９号の各公報に示された技術がある。

【０００５】

【発明が解決しようとする課題】上記各従来技術は、認証を経ないとプリントサーバから印刷出力が行われないため、印刷結果の秘密保護という面では有効であった。しかしながら、上記各従来技術はいずれも、クライアントから送られてきた印刷データをプリントサーバ内にそのまま保管するため、保管した印刷データを覗き見られる可能性があった。

【０００６】本発明はこのような問題を解決するためになされたものであり、プリンタなどの画像出力装置に保管したデータの秘密保護を実現する画像出力制御方法及び装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】このような問題を解決するために、本発明では、プリンタなどの画像出力装置に対し、暗号化処理を施した画像出力ジョブを保管するようにする。そして、印刷などの画像出力の際には、保管したジョブデータを、ユーザが入力した復号キーにより復号化し、出力処理を行う。

【０００８】ここで、復号化結果が正しいか否かを判定し、正しくない場合には出力処理を行わないようにすることで、無駄な出力を防止できる。なお、復号化結果の適否の判定は、例えば、暗号化の際に元のジョブのデータから照合用データを作成して保管し、復号化結果をその照合用データと比較したり、あるいは照合用データをジョブのデータに付加して暗号化し、復号化結果でその照合用データが正しく復号されているかを調べたりすることにより行うことができる。

【０００９】

【発明の実施の形態】以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。

【００１０】［実施形態１］図１は、本発明の第１の実施形態を説明するための図である。

【００１１】このシステムにおいて、画像出力装置としてのプリンタシステム１０は、例えばプリントショップやオフィスなどに置かれる共用のプリンタシステムであり、プリントサーバ１２、記憶装置１４、プリントエンジン１６及びＵＩ（ユーザインタフェース）部１８を含む。

【００１２】プリントサーバ１２は、プリンタシステム１０の全体的な処理の制御を行う装置である。プリントサーバ１２は、クライアント装置２０からの印刷指示の受け付けや、印刷ジョブのスケジューリング、印刷データの印刷可能形式への変換などの一般的な処理機能に加え、記憶装置１４に対して印刷データを暗号化して保管する機能を備える。記憶装置１４は、クライアント装置２０から受け取った印刷データ等を蓄積する装置である。プリントエンジン１６は、印刷データを紙などに印刷する装置である。ＵＩ部１８は、ユーザに対して、プリンタシステム１０の操作メニューや状態表示などを提供し、指示入力等を受け付ける装置である。

【００１３】プリンタシステム１０は、クライアント装置２０から受信した印刷データ１００を、ユーザからの出力指示が有るまで保管する機能を有する。ここで、本実施形態では、印刷データをそのまま保管するのではなく、暗号化を施して保管することにより、保管中の印刷データの秘密保護を図る。暗号化処理はプリントサーバ１２が行い、暗号化のための暗号鍵には、クライアント装置２０から供給される認証コード１２０を用いる。

【００１４】ユーザＡは、プリンタシステム１０から印刷データ１００を印刷出力しようとする際、印刷データの秘密保護を望む場合には、認証コード１２０を設定する。認証コード１２０の設定は、ユーザＡ自身が入力する方式、ユーザの指示に応じてクライアント装置２０が自動生成する方式のいずれでもよい。設定された認証コード１２０は、印刷データ１００と対応づけて、プリンタシステム１０に送信される。また、送信される印刷データ１００には、識別情報１１０が付加される。この識別情報１１０は、例えば印刷データ１００のタイトルなど、ユーザＡが印刷データ１００を識別するための情報であり、認証コード１２０の設定の有無にかかわらず設定される。

【００１５】クライアント装置２０から印刷データ１００を受信したプリンタシステム１０では、プリントサーバ１２がこの印刷データ１００を、対応する識別情報１１０とともに記憶装置１４に記憶する。この処理手順を図２に示す。

【００１６】プリントサーバ１２は、通常は、印刷データ１００、識別情報１１０及び認証コード１２０等のデータの受信待ち状態となっている（Ｓ１０，Ｓ１２）。印刷データ１００を受信すると、認証コード１２０が付随しているかどうかを調べる（Ｓ１４）。認証コード１２０がなければ、（ユーザが秘密保護を要求していないということなので）プリントサーバ１２は、識別情報１１０に対応づけてその印刷データ１００をそのまま保管データ１５０として記憶装置１４に保管する（Ｓ２４）。

【００１７】認証コード１２０があれば、次にプリントサーバ１２は、その印刷データ１００が、プリントエンジン１６で処理可能なＰＤＬ（ページ記述言語）のデータか否かを判定する（Ｓ１６）。この判定結果がＮｏであれば、プリントサーバ１２はその印刷データ１００をＰＤＬに変換する（Ｓ１８）。印刷データ１００がＰＤＬであれば、この変換は不要である。

【００１８】次にプリントサーバ１２は、ＰＤＬの印刷データから照合用データ１６０を作成し、識別情報１１０と対応づけて保存する（Ｓ２０）。照合用データ１６０は、そのＰＤＬデータのヘッダ等の所定の一部分（印刷内容と関係ない部分が望ましい）を抽出したものや、そのＰＤＬデータのチェックサム値など、そのＰＤＬデータから所定の規則に基づいて作成する。そして、認証コード１２０をキーとして用い、ＰＤＬの印刷データを暗号化し（Ｓ２２）、その暗号化したデータを保管データ１５０として、識別情報１１０に対応づけて記憶装置１４に保管する（Ｓ２４）。保管が完了すると、元の印刷データ１００及び認証コード１２０は破棄される。

【００１９】次に、このようにして保管したデータ１５０を印刷出力するときの処理を図３を参照して説明する。

【００２０】まず、プリントサーバ１２は、記憶装置１４内に保管している保管データ１５０の識別情報１１０の一覧を、ＵＩ部１８に表示する（Ｓ３０）。プリンタシステム１０のところまで来たユーザＡは、ＵＩ部１８にてその一覧表示の中から、印刷出力したいデータを選択して指示する（Ｓ３２）。これに応じて、プリントサーバ１２は印刷開始の確認表示をＵＩ部１８に行い、ユーザはそのデータでよければその旨をＵＩ部１８に入力する（Ｓ３４）。

【００２１】ユーザが確認すると、プリントサーバ１２は、その選択された保管データ１５０が暗号化されているデータか否かチェックする（Ｓ３６）。暗号化されていなければ、プリントサーバ１２は、その保管データをそのままプリントエンジン１６に渡し、印刷出力させる（Ｓ４４）。暗号化されていれば、プリントサーバ１２は、認証コードの入力を促す表示をＵＩ部１８に行い、それに対するユーザからの認証コードの入力を受け付ける（Ｓ３８）。

【００２２】認証コードの入力方式は、キーパッドやタッチパネルなどでユーザが手入力で行う方式の他にも、ＩＣカードやメモリカードなどの携帯記憶媒体に認証コードを記憶させ、プリンタシステム１０にその記憶媒体を読み取る読み取り装置を設ける方式も好適である。

【００２３】認証コードが入力されると、プリントサーバ１２は、そのコードを用いて保管データ１５０を復号化する（Ｓ４０）。そして、その保管データ１５０に対応して保管していた照合用データ１６０とその復号結果とを照合し、正しく復号されているかどうかをチェックする（Ｓ４２）。正しく復号されていなければ、Ｓ３８に戻り、認証コードの再入力を行う。照合の結果、正しく復号されていれば、その復号結果のデータ（ＰＤＬのデータ）をプリントエンジン１６に渡して印刷出力を行わせる（Ｓ４４）。これにより印刷結果２００が得られる。

【００２４】Ｓ４４の印刷出力の後、プリントサーバ１２は、ＵＩ部１８を介してユーザに対し、印刷出力した保管データ１５０を破棄するか否かを問い合わせる（Ｓ４６）。保管データ１５０の再利用の予定があるなどの場合には、ユーザは破棄しない旨の指示を入力すればよい。破棄の指示があった場合には、プリントサーバ１２は、その保管データ１５０（及び対応する識別情報１１０と照合データ１６０（もしあれば））を記憶装置１４から削除する（Ｓ４８）。破棄しない旨の指示があれば、削除は行わない。なお、保管データ１５０を残せるようにするのは、オフィスビルなどでの用途では有用であるが、プリントショップなどに設置するシステムの場合には必要ない。

【００２５】なお、印刷出力時の印刷属性（部数や片面／両面など）は、クライアント装置２０にて設定して印刷データ１００に付加して送信してもよいし、プリンタシステム１０側で、例えば認証（復号）成功後などに、入力できるようにしてもよい。

【００２６】以上説明したように、本実施形態のシステムによれば、プリンタシステム１０に、印刷データ１００を暗号化して保管することができるので、保管中のデータを万が一覗き見られても、その内容を知られるおそれがない。また、本実施形態の仕組みは、正しい認証コードにより保管データが正しく復号されないと印刷出力が行われないので、出力指示時のユーザ認証の機能も果たしている。また、正しく復号されないと、印刷出力が行われず保管データの破棄も行われないので、正しくない復号結果のまま印刷出力されて保管データが削除されてしまうようなこともない。

【００２７】なお、以上の例では、暗号化前の印刷データ（ＰＤＬ）から照合用データ１６０を作成したが、印刷データとはまったく無関係に照合用データ１６０を自動生成し、これを印刷データに付加して暗号化を行ってもよい。また、照合用データを固定値とし、これを印刷データに付加して暗号化してもよい。この場合、照合用データを保管データ１５０に対応づけて保存する必要がない。

【００２８】また、以上の例では、暗号化及び復号化を同じ認証コードで行ったが、公開鍵暗号方式などを利用すれば、暗号化のキーと復号化のキーを別々にすることもできる。

【００２９】また、以上の例では、プリントサーバ１２は、受信した印刷データ１００をプリントエンジン１６が処理可能なＰＤＬに変換してから保管のための暗号化を行ったが、受信した印刷データ１００を認証コード１２０で暗号化して保管することも好適である。この場合、ユーザの認証コード入力により復号化処理を行った後、ＰＤＬへの変換が行われる。

【００３０】［実施形態２］上記実施形態１は、プリンタシステム１０側で印刷データを暗号化した。これに対して、本実施形態では、クライアント装置２０側で暗号

化したデータをプリンタシステム１０に保管する方式を採用した。

【００３１】図４に、本実施形態のシステムの概念図を示す。本実施形態では、クライアント装置２０とプリンタシステム１０とに同じ暗号方式（アルゴリズム）を搭載する。そして、ユーザＡは、印刷データの秘密保護を望む場合には、クライアント装置２０上で所望の認証コードを用いてその印刷データを暗号化し、得られた暗号化データ１８０をプリンタシステム１０に送る。

【００３２】送信する暗号化データ１８０には、プリンタシステム１０側での復号結果のチェックのために、チェックサムなどの照合用データ１６０を付加し、更に識別情報１１０と認証フラグ１７０を付加する。認証フラグ１７０は、送信する印刷データが認証を要するものの暗号化データ１８０であるか、それとも暗号化されてないＰＤＬやアプリケーションのデータであるかを示すフラグである。これは、プリンタシステム１０が、受信したデータに復号処理が必要か否かを判別するために用いる。なお、プリンタシステム１０が、ファイル名その他の属性情報により復号処理の要否を判別できるのであれば、認証フラグ１７０は必要ない。

【００３３】図４では図示を省略したが、クライアント装置２０から送信する印刷データが秘密保護の必要のないものの場合は、照合用データ１６０は付加されず、認証フラグ１７０は認証（復号・照合）不要を示す値に設定されている。

【００３４】クライアント装置２０から、印刷依頼のデータを受信したプリントサーバ１２は、それらの情報を記憶装置１４に保管する。そして、ＵＩ部１８にそれら保管データの識別情報１１０の一覧を表示し、ユーザからの選択を待つ。

【００３５】ユーザがデータを選択した場合、プリントサーバ１２は、そのデータの認証フラグ１７０を調べる。その結果、認証が不要であれば、そのデータを、プリントエンジン１６が処理可能なＰＤＬの形に変換し、プリントエンジン１６から印刷出力させる。一方、認証が必要であれば、ユーザに認証コードの入力を促し、これに応じて入力された認証コードをキーとして暗号化データ１８０を復号化する。そして、その復号結果が正しいものであるかどうかを、照合用データ１６０を用いて検査する。以降、実施形態１と同様の処理が行われ、復号結果が正しい場合は印刷出力が行われる。

【００３６】このように、本実施形態では、認証コード（暗号鍵）を直接プリンタシステム１０に渡さなくてよいので、よりセキュリティが向上する。

【００３７】［実施形態３］以上の各実施形態は、認証コード（暗号鍵）をユーザ側で設定していた。これに対して本実施形態では、プリンタシステム１０側で認証コードを設定し、これをユーザ側に通知する方式を採る。以下、ユーザがクライアント装置として携帯端末２０ａを持ち、電子メールを用いて印刷等の指示を行う場合の実施例を説明する。

【００３８】ユーザは、印刷したい場合、（１）印刷データ３０２を含んだ電子メール３００を携帯端末２０ａからプリンタシステム１０に送る。印刷データ３０２は、例えば電子メールの本文や添付ファイルなどの形で電子メール３００に組み込まれる。

【００３９】これを受けたプリンタシステム１０のプリントサーバ１２は、その電子メール３００での印刷依頼に対して認証コード３１２と識別情報３１４を付与する。そして、プリントサーバ１２は、実施形態１と同様、照合用データ３６０を電子メール３００中の印刷データ３０２から生成し、これを識別情報３１４と対応づけて記憶装置１４に記憶する。また、プリントサーバ１２は、付与した認証コード３１２により、印刷データ３０２を暗号化し、その暗号化結果を保管データ３５０として、識別情報３１４に対応づけて記憶装置１４に保管する。そして、（２）プリントサーバ１２は、印刷依頼メールの送信元の携帯端末２０ａに対して、識別情報３１４と認証コード３１２を含んだ電子メール３１０を返信する。このメール３１０は、プリンタシステム１０が印刷依頼を受け付けた旨のメッセージを含んでいてもよい。

【００４０】そして、ユーザはプリンタシステム１０のところまで移動すると、携帯端末２０ａから、（３）先ほどのプリンタシステム１０からの電子メール３１０に対して返信を行う。返信のメールに元のメッセージを残すよう携帯端末２０ａの搭載するメールシステムに設定しておけば、返信される電子メール３２０には、認証コード３１２と識別情報３１４が自動的に組み込まれる。ユーザはそれら認証コード３１２などを改めて手入力する必要がない。

【００４１】このメール３２０を受け取ったプリントサーバ１２は、そのメール３２０から識別情報３１４及び認証コード３１２を抽出し、その識別情報３１４に対応する保管データ３５０及び照合用データ３６０を記憶装置１４から取り出す。そして、プリントサーバ１２は、その保管データ３５０を認証コード３１２をキーとして復号し、その復号結果の適否をその照合用データ３６０により判定する。そして、復号結果が正しい場合にはプリントエンジン１６に印刷を行わせ、復号結果が正しくない場合にはユーザに対してエラーの旨を通知するメールを送信する。

【００４２】このように、本実施形態では、実施形態１等と同様の効果が得られるとともに、電子メールの仕組みを利用することにより、出力指示の際のユーザの入力の手間を省くことができる。ユーザ側の装置には、標準的なメーラー・ソフトウエアさえ搭載されていればよく、この仕組みのための特別のハードウエアやソフトウエアを設ける必要がない。

【図面の簡単な説明】

【図１】　実施形態１のシステムを説明するための図である。

【図２】　プリントサーバのデータ受信時の動作を示すフローチャートである。

【図３】　プリントサーバの出力指示受付時の動作を示すフローチャートである。

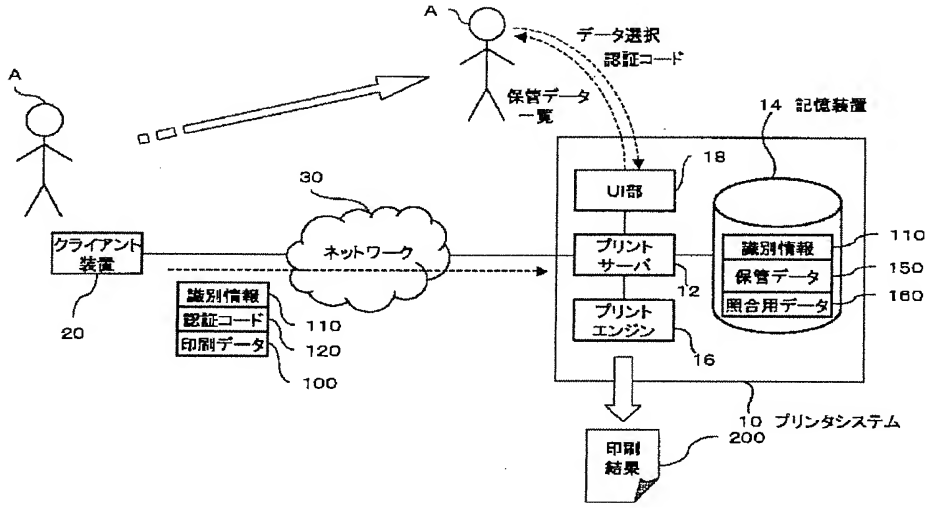
【図４】　実施形態２のシステムを説明するための図である。

＊【図５】　実施形態３のシステムを説明するための図である。

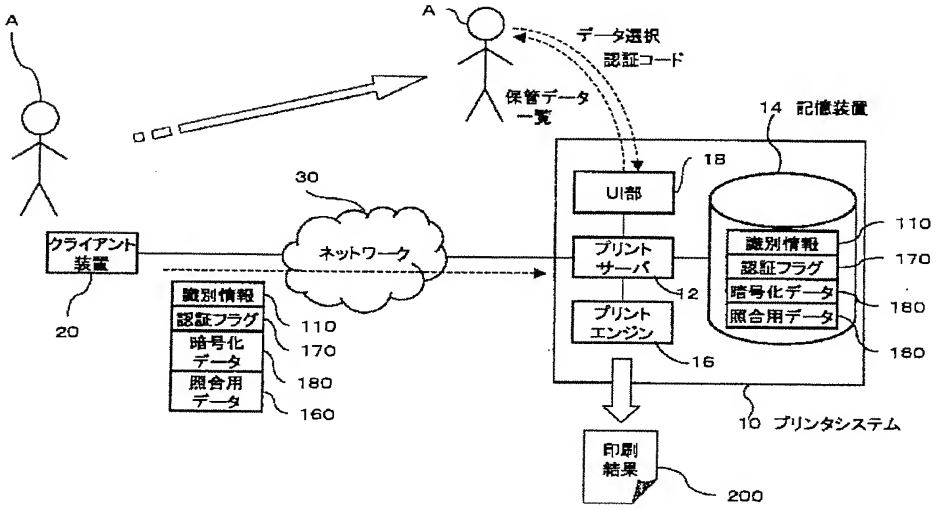
【符号の説明】

１０　プリンタシステム、１２　プリントサーバ、１４　記憶装置、１６　プリントエンジン、１８　ＵＩ部、２０　クライアント装置、３０　ネットワーク、１００　印刷データ、１１０　識別情報、１２０　認証コード、１５０　保管データ、１６０　照合用データ。

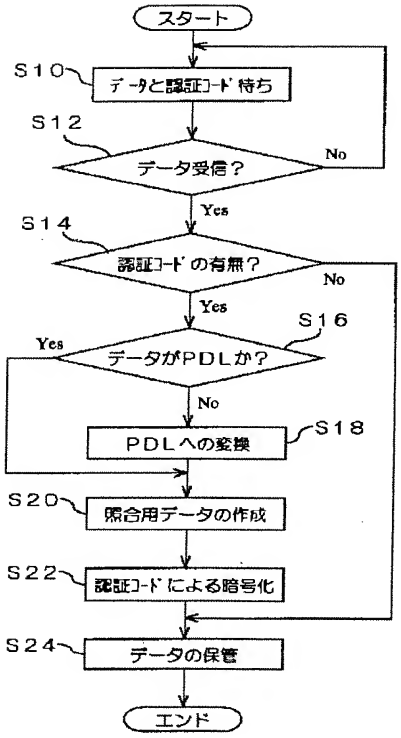
【図１】



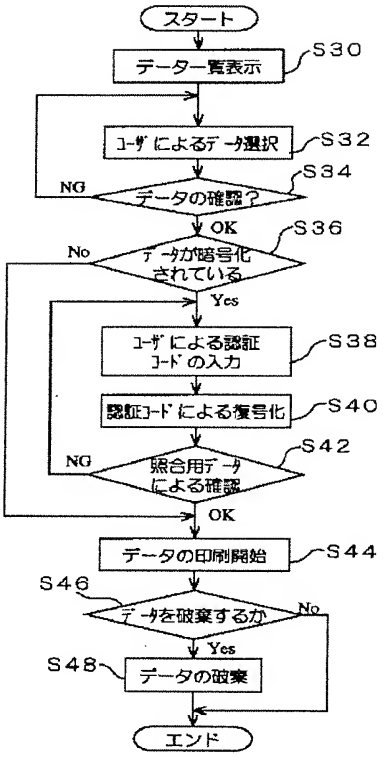
【図４】



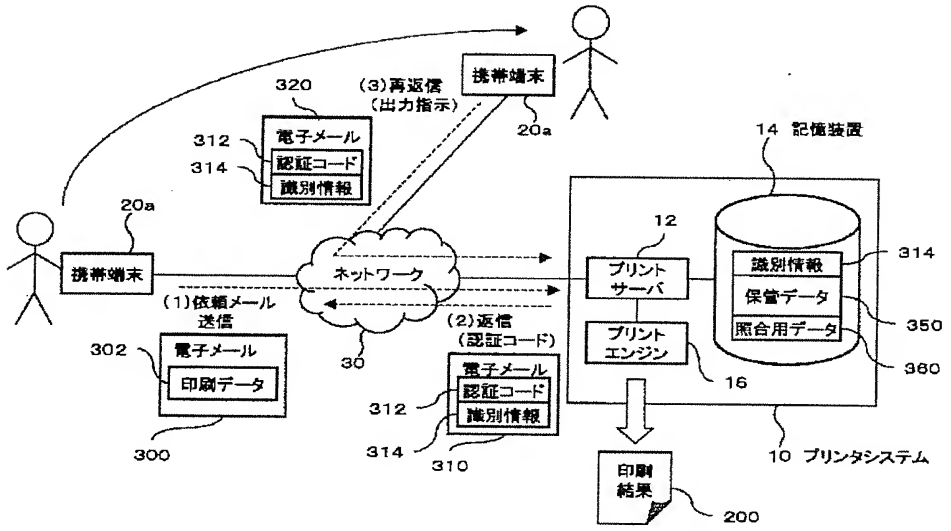
【図２】


スタート
S10
データと認証コード待ち
S12
データ受信？
No
Yes
S14
認証コードの有無？
No
Yes
S16
Yes
データがPDLか？
No
S18
PDLへの変換
S20
照合用データの作成
S22
認証コードによる暗号化
S24
データの保管
エンド

【図３】


スタート
S30
データー覧表示
S32
ユーザによるデータ選択
S34
NG
データの確認？
OK
S36
No
データが暗号化されている
Yes
S38
ユーザによる認証コードの入力
S40
認証コードによる復号化
S42
NG
照合用データによる確認
OK
S44
データの印刷開始
S46
データを破棄するか
No
Yes
S48
データの破棄
エンド

【図５】


携帯端末
20a
(3)再返信
(出力指示)
320
電子メール
312
認証コード
314
識別情報
14 記憶装置
12
プリント
サーバ
識別情報
保管データ
照合用データ
314
350
360
プリント
エンジン
16
ネットワーク
(1)依頼メール
送信
(2)返信
(認証コード)
30
302
電子メール
印刷データ
300
電子メール
認証コード
識別情報
312
314
310
10 プリンタシステム
印刷
結果
200

フロントページの続き

(72)発明者　源田　公平
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル
富士ゼロックス株式会社内
(72)発明者　土岐　康之
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル
富士ゼロックス株式会社内

Ｆターム(参考)　2C087 BA01 BA14 BB03 BC07 CB10
CB12 DA13 DA14
5B021 AA01 BB01 BB04 CC00
5J104 AA01 AA07 KA01 NA02 PA07
PA14
9A001 BB04 BB06 CC02 EE03 FF01
JJ14 JJ27 KK42 LL03